

PATENT ABSTRACTS OF JAPAN

(11)Publication number : 2000-322381

(43)Date of publication of application : 24.11.2000

(51)Int.Cl.

G06F 15/00

(21)Application number : 11-134190

(71)Applicant : MITSUBISHI ELECTRIC CORP

(22)Date of filing : 14.05.1999

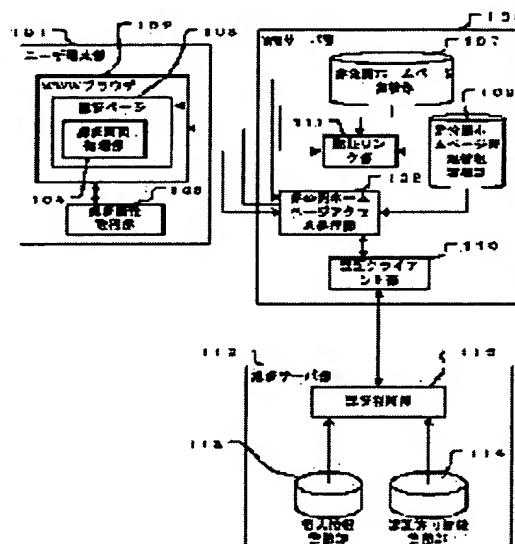
(72)Inventor : SUZUKI YUMIKO
NAKAMURA HIROSHI
SADAKANE TETSUO

(54) DEVICE AND METHOD FOR CONTROLLING HOMEPAGE ACCESS

(57)Abstract:

PROBLEM TO BE SOLVED: To change authentication types in each prescribed group such as a homepage content by providing an authentication allowance information storing part in which an access control ID and an authentication type are associated and stored.

SOLUTION: In an authentication server part 112, an authentication deciding part 115 receives authentication information, an access control ID and an authentication client ID transmitted from an authentication client part 110 and detects an authentication type corresponding to a user ID, the access control ID and the authentication client ID included in the authentication information from an authentication allowance information storing part 114. The part 114 stores authentication allowance information obtained by making the access control ID correspond to the authentication type used for authentication processing. Grouping is performed by combining the user ID, the authentication client ID and the access control ID, and authentication types can be changed in accordance with the group.



LEGAL STATUS

[Date of request for examination]

[Date of sending the examiner's decision of rejection]

[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]

[Date of final disposal for application]

[Patent number]

[Date of registration]

[Number of appeal against examiner's decision of rejection]

[Date of requesting appeal against examiner's decision of rejection]

[Date of extinction of right]

Copyright (C); 1998,2003 Japan Patent Office

(19)日本国特許庁 (J P)

(12) 公 開 特 許 公 報 (A)

(11)特許出願公開番号
特開2000-322381
(P2000-322381A)

(43)公開日 平成12年11月24日(2000.11.24)

(51)Int.Cl.⁷

G 0 6 F 15/00

識別記号

3 3 0

F I

G 0 6 F 15/00

テーマコード(参考)

3 3 0 D 5 B 0 8 5

審査請求 未請求 請求項の数 3 O L (全 13 頁)

(21)出願番号 特願平11-134190

(22)出願日 平成11年5月14日(1999.5.14)

(71)出願人 000006013

三菱電機株式会社

東京都千代田区丸の内二丁目2番3号

(72)発明者 鈴木 由美子

東京都千代田区丸の内二丁目2番3号 三
菱電機株式会社内

(72)発明者 中村 浩

東京都千代田区丸の内二丁目2番3号 三
菱電機株式会社内

(74)代理人 100102439

弁理士 宮田 金雄 (外2名)

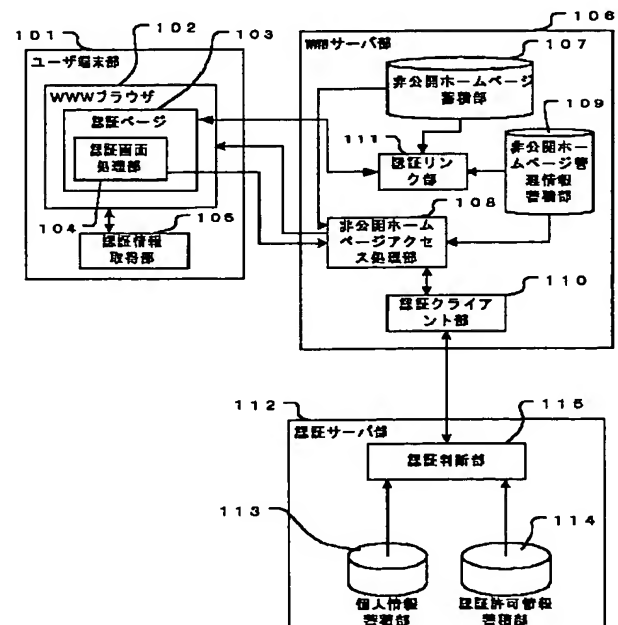
最終頁に続く

(54)【発明の名称】 ホームページアクセス制御装置およびホームページアクセス制御方法

(57)【要約】

【課題】 所定グループ毎に認証種類を変えられると共に、セキュリティ性の高いホームページアクセス制御装置およびホームページアクセス制御方法を得る。

【解決手段】 ユーザ端末部とWWWサーバ部と認証サーバ部で構成され、WWWサーバ部は、グループ化された複数のホームページが蓄積された非公開ホームページ蓄積部と、ホームページのページIDと属するグループのアクセス制御IDとが格納された非公開ホームページ管理情報蓄積部と、アクセス制御IDとユーザの認証情報とを認証サーバ部に送付するアクセス部とを有し、認証サーバ部は、ユーザの認証情報が格納された個人情報蓄積部と、アクセス制御IDと認証の種類とが格納された認証許可情報蓄積部と、アクセス制御IDに対応する認証の種類に応じた認証情報を個人情報蓄積部から検出し、サーバ部から受け付けた認証情報とを比較して認証判断する認証判断部とを有する。



【特許請求の範囲】

【請求項 1】 ホームページを公開する WWWサーバ部と上記ホームページをアクセスするユーザ端末部と上記ホームページをアクセスするユーザの認証を行う認証サーバ部で構成されるホームページアクセス制御装置において、

上記ユーザ端末部は、上記ホームページを表示する WWWブラウザと、上記ユーザの認証情報を取得する認証情報取得部と、当該認証情報取得部が取得した認証情報と上記ユーザ所望のホームページのページ ID とを上記 WWWサーバ部に送付する認証画面処理部とを有し、
上記 WWWサーバ部は、所定のグループにグループ化され、特定ユーザのみに公開される複数のホームページが蓄積された非公開ホームページ蓄積部と、上記複数のホームページのそれぞれのページ ID と上記ホームページがそれぞれ属するグループのアクセス制御 ID とが対応づけられて格納された非公開ホームページ管理情報蓄積部と、上記ユーザ端末部から送付された上記ユーザ所望のホームページのページ ID と上記ユーザの認証情報とを受け付け、上記非公開ホームページ管理情報蓄積部から上記ユーザ所望のホームページのページ ID に対応づけられた上記アクセス制御 ID を検出し、当該検出したアクセス制御 ID と上記ユーザの認証情報とを上記認証サーバ部に送付して認証要求し、当該認証結果が認証 OK の場合に上記非公開ホームページ蓄積部から上記ユーザ所望のホームページを検出して上記ユーザ端末に送付するアクセス部とを有し、

上記認証サーバ部は、上記ユーザの予め登録された認証情報が格納された個人情報蓄積部と、上記アクセス制御 ID と認証処理に用いられる認証の種類とが対応づけられて格納された認証許可情報蓄積部と、上記 WWWサーバ部から送付された上記アクセス制御 ID と上記ユーザの認証情報とを受け付け、上記認証許可情報蓄積部から上記アクセス制御 ID に対応づけられた認証の種類を検出し、上記個人情報蓄積部から上記検出した認証の種類に応じた上記ユーザの認証情報を検出し、当該検出した認証情報と上記 WWWサーバ部から受け付けた認証情報とを比較して認証判断し、当該認証結果を上記 WWWサーバ部に送付する認証判断部とを有したことを特徴とするホームページアクセス制御装置。

【請求項 2】 上記 WWWサーバ部の上記アクセス部は、上記ユーザ端末にホームページを送付する際に当該ホームページが属するグループのアクセス制御 ID を上記ユーザ端末に送付するように構成され、
上記ユーザ端末部は、上記アクセス部から送付されたホームページにリンクされた上記ユーザ所望の次のホームページのページ ID と上記アクセス部から送付されたアクセス制御 ID とを上記 WWWサーバ部に送付するように構成され、

さらに、上記 WWWサーバ部は、上記ユーザ端末部から

送付された上記次のホームページのページ ID と上記アクセス制御 ID とを受け付け、上記非公開ホームページ管理情報蓄積部から上記次のホームページのページ ID に対応づけられたアクセス制御 ID を検出し、当該検出したアクセス制御 ID と上記ユーザ端末部から送付されたアクセス制御 ID とを比較し、一致する場合に上記非公開ホームページ蓄積部から上記次のホームページを検出して上記ユーザ端末部に送付する認証リンク部を有したことを特徴とする請求項 1 に記載のホームページアクセス制御装置。

【請求項 3】 ホームページを公開する WWWサーバ部と上記ホームページをアクセスするユーザ端末部と上記ホームページをアクセスするユーザの認証を行う認証サーバ部で構成されるホームページアクセス制御装置を用いたホームページアクセス制御方法において、
上記ユーザ端末部で、上記ホームページを表示する WWWブラウザステップと、上記ユーザの認証情報を取得する認証情報取得ステップと、当該認証情報取得ステップで取得した認証情報と上記ユーザ所望のホームページのページ ID とを上記 WWWサーバ部に送付する認証画面処理ステップとを実行し、

上記 WWWサーバ部で、上記ユーザ端末部から送付された上記ユーザ所望のホームページのページ ID と上記ユーザの認証情報とを受け付ける WWW受け付けステップと、所定のグループにグループ化され、特定ユーザのみに公開される複数のホームページのそれぞれのページ ID と上記ホームページがそれぞれ属するグループのアクセス制御 ID とが対応づけられて格納された非公開ホームページ管理情報蓄積部から上記ユーザ所望のホームページのページ ID に対応づけられた上記アクセス制御 ID を検出する WWW検出ステップと、当該 WWW検出ステップで検出したアクセス制御 ID と上記ユーザの認証情報とを上記認証サーバ部に送付して認証要求する認証要求ステップと、上記認証の結果が認証 OK の場合に上記ユーザ所望のホームページを上記非公開ホームページ蓄積部から検出して上記ユーザ端末に送付する WWW送付ステップとを実行し、

上記認証サーバ部で、上記 WWWサーバ部から送付された上記アクセス制御 ID と上記ユーザの認証情報とを受け付ける認証受け付けステップと、上記アクセス制御 ID と認証処理に用いられる認証の種類とが対応づけられて格納された認証許可情報蓄積部から上記認証受け付けステップで受け付けたアクセス制御 ID に対応づけられた認証の種類を検出し、上記ユーザの予め登録された認証情報が格納された個人情報蓄積部から上記検出された認証の種類に応じた上記ユーザの認証情報を検出する認証検出ステップと、当該認証検出ステップで検出した認証情報と上記 WWWサーバ部から受け付けた認証情報とを比較して認証判断する認証判断ステップと、当該認証判断ステップの認証結果を上記 WWWサーバ部に送付する認

証送付ステップとを実行したことを特徴とするホームページアクセス制御方法。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】この発明は、ホームページを公開するWWWサーバ部と上記ホームページをアクセスするユーザ端末部と上記ホームページをアクセスするユーザの認証を行う認証サーバ部で構成されるホームページアクセス制御装置およびこのホームページアクセス制御装置を用いたホームページアクセス制御方法に関するものである。

【0002】

【従来の技術】図10は例えば、日経BP社が発行するNECイントラネットプロジェクト編「イントラネット完全構築ガイド」(1996年)の278頁から290頁に示された従来のWWWシステムによるホームページアクセス制御装置を示す構成図である。

【0003】図10において、101はユーザ端末部、102はWWWブラウザ、1001はWWWサーバ部106上の非公開情報(ホームページ)にアクセスするために上記WWWサーバ部106からユーザ端末部101にダウンロードされた利用者認証ページ、1002は認証の結果に応じて上記WWWサーバ部106から返信された返信ホームページ、106はWWWサーバ部、1003は上記WWWサーバ部106上で非公開情報(ホームページ)へのアクセス制御を行うアクセス制御処理部、1004は非公開情報(ホームページ)蓄積部、1005は利用者の認証を行う認証処理部、1006は利用者の認証に必要な予め登録された認証情報を保持する利用者管理情報蓄積部、1007は上記返信ホームページ1002として公開された非公開情報(ホームページ)よりリンクされた別の非公開情報(ホームページ)を表示するリンク部である。

【0004】次に動作について説明する。利用者がWWWサーバ部106上の非公開情報(ホームページ)にアクセスする際に、まず、利用者認証を行うための利用者認証ページ1001がユーザ端末部101にダウンロードされ、WWWブラウザ102に表示される。上記利用者はこの利用者認証ページ1001にユーザIDやパスワード等の予め定められた所定の認証情報を入力し、WWWサーバ部106に送信する。WWWサーバ部106では、アクセス制御処理部1003が上記ユーザ端末部101から送信された上記認証情報を受け取り、認証処理部1005に利用者の認証を依頼する。

【0005】認証処理部1005は利用者管理情報蓄積部1006で保持している予め登録されたユーザIDやパスワード等の認証情報と、上記ユーザ端末部101から送信された認証情報とを照合し、利用者の認証を行い、その認証結果をアクセス制御処理部1003に送る。アクセス制御処理部1003は、認証結果が認証O

Kの場合は、上記利用者が目的とする非公開情報(ホームページ)をWWWブラウザ102に送付し、認証NGの場合はエラーメッセージ等の情報をWWWブラウザ102に送付し、返信ホームページ1002として表示させる。ここで、上記返信ホームページ1002には認証されたことを示すトークンが設定されている。上記利用者がこの返信ホームページとして表示された非公開情報(ホームページ)のリンクをたどり次の非公開情報(ホームページ)を参照する場合は、上記トークンと上記利用者が目的とする次の非公開情報(ホームページ)への指定情報とがリンク部1007に送付される。当該リンク部1007は、上記トークンの有効性をチェックして、有効な場合は上記指定された非公開情報(ホームページ)を返信ホームページとしてブラウザ102に送付し、表示させる。

【0006】このように、従来のWWWシステムによるホームページアクセス制御装置およびその制御方法では、利用者がWWWサーバ部上の非公開情報にアクセスするときに、ユーザ端末部から送信された上記利用者の認証情報と、予め利用者管理情報蓄積部に登録された認証情報とを照合して利用者の認証を行うことにより、公開可能な利用者を限定するような制御を行うことができる。

【0007】

【発明が解決しようとする課題】しかしながら、従来のホームページアクセス制御では、上記認証処理部は予め定められた認証の種類で認証を行うため、例えば、非公開情報(ホームページ)の内容に応じて認証の種類を変えることができないという問題があった。

【0008】また、一度認証が行われ非公開情報(ホームページ)にアクセスすると、その非公開情報(ホームページ)からリンクが張られている次の非公開情報(ホームページ)に対して、その非公開情報(ホームページ)の内容に関わらず、新たに認証を行うことなくアクセス可能になってしまうという問題があった。

【0009】この発明は上記のような問題点を解決するためになされたもので、例えば、ホームページの内容等の所定のグループ毎に認証の種類を変えることができると共に、セキュリティ性の高いホームページアクセス制御装置およびホームページアクセス制御方法を得ることを目的とする。

【0010】

【課題を解決するための手段】この発明に係るホームページアクセス制御装置は、ホームページを公開するWWWサーバ部と上記ホームページをアクセスするユーザ端末部と上記ホームページをアクセスするユーザの認証を行う認証サーバ部で構成されるホームページアクセス制御装置であって、上記ユーザ端末部は、上記ホームページを表示するWWWブラウザと、上記ユーザの認証情報を取得する認証情報取得部と、当該認証情報取得部が取

得した認証情報と上記ユーザ所望のホームページのページIDとを上記WWWサーバ部に送付する認証画面処理部とを有し、上記WWWサーバ部は、所定のグループにグループ化され、特定ユーザのみに公開される複数のホームページが蓄積された非公開ホームページ蓄積部と、上記複数のホームページのそれぞれのページIDと上記ホームページがそれぞれ属するグループのアクセス制御IDとが対応づけられて格納された非公開ホームページ管理情報蓄積部と、上記ユーザ端末部から送付された上記ユーザ所望のホームページのページIDと上記ユーザの認証情報とを受け付け、上記非公開ホームページ管理情報蓄積部から上記ユーザ所望のホームページのページIDに対応づけられた上記アクセス制御IDを検出し、当該検出したアクセス制御IDと上記ユーザの認証情報とを上記認証サーバ部に送付して認証要求し、当該認証結果が認証OKの場合に上記非公開ホームページ蓄積部から上記ユーザ所望のホームページを検出して上記ユーザ端末部に送付するアクセス部とを有し、上記認証サーバ部は、上記ユーザの予め登録された認証情報が格納された個人情報蓄積部と、上記アクセス制御IDと認証処理に用いられる認証の種類とが対応づけられて格納された認証許可情報蓄積部と、上記WWWサーバ部から送付された上記アクセス制御IDと上記ユーザの認証情報とを受け付け、上記認証許可情報蓄積部から上記アクセス制御IDに対応づけられた認証の種類を検出し、上記個人情報蓄積部から上記検出した認証の種類に応じた上記ユーザの認証情報を検出し、当該検出した認証情報と上記WWWサーバ部から受け付けた認証情報とを比較して認証判断し、当該認証結果を上記WWWサーバ部に送付する認証判断部とを有したものである。

【0011】また、次の発明に係るホームページアクセス制御装置は、上記WWWサーバ部の上記アクセス部は、上記ユーザ端末にホームページを送付する際に当該ホームページが属するグループのアクセス制御IDを上記ユーザ端末に送付するように構成され、上記ユーザ端末部は、上記アクセス部から送付されたホームページにリンクされた上記ユーザ所望の次のホームページのページIDと上記アクセス部から送付されたアクセス制御IDとを上記WWWサーバ部に送付するように構成され、さらに、上記WWWサーバ部は、上記ユーザ端末部から送付された上記次のホームページのページIDと上記アクセス制御IDとを受け付け、上記非公開ホームページ管理情報蓄積部から上記次のホームページのページIDに対応づけられたアクセス制御IDを検出し、当該検出したアクセス制御IDと上記ユーザ端末部から送付されたアクセス制御IDとを比較し、一致する場合に上記非公開ホームページ蓄積部から上記次のホームページを検出して上記ユーザ端末部に送付する認証リンク部を有したものである。

【0012】さらにまた、次の発明に係るホームページ

アクセス制御方法は、ホームページを公開するWWWサーバ部と上記ホームページをアクセスするユーザ端末部と上記ホームページをアクセスするユーザの認証を行う認証サーバ部で構成されるホームページアクセス制御装置を用いたホームページアクセス制御方法であって、上記ユーザ端末部で、上記ホームページを表示するWWWブラウザステップと、上記ユーザの認証情報を取得する認証情報取得ステップと、当該認証情報取得ステップで取得した認証情報と上記ユーザ所望のホームページのページIDとを上記WWWサーバ部に送付する認証画面処理ステップとを実行し、上記WWWサーバ部で、上記ユーザ端末部から送付された上記ユーザ所望のホームページのページIDと上記ユーザの認証情報とを受け付けるWWW受付ステップと、所定のグループにグループ化され、特定ユーザのみに公開される複数のホームページのそれぞれのページIDと上記ホームページがそれぞれ属するグループのアクセス制御IDとが対応づけられて格納された非公開ホームページ管理情報蓄積部から上記ユーザ所望のホームページのページIDに対応づけられた上記アクセス制御IDを検出するWWW検出ステップと、当該WWW検出ステップで検出したアクセス制御IDと上記ユーザの認証情報とを上記認証サーバ部に送付して認証要求する認証要求ステップと、上記認証の結果が認証OKの場合に上記ユーザ所望のホームページを上記非公開ホームページ蓄積部から検出して上記ユーザ端末部に送付するWWW送付ステップとを実行し、上記認証サーバ部で、上記WWWサーバ部から送付された上記アクセス制御IDと上記ユーザの認証情報とを受け付ける認証受付ステップと、上記アクセス制御IDと認証処理に用いられる認証の種類とが対応づけられて格納された認証許可情報蓄積部から上記認証受付ステップで受け付けたアクセス制御IDに対応づけられた認証の種類を検出し、上記ユーザの予め登録された認証情報が格納された個人情報蓄積部から上記検出された認証の種類に応じた上記ユーザの認証情報を検出する認証検出ステップと、当該認証検出ステップで検出した認証情報と上記WWWサーバ部から受け付けた認証情報とを比較して認証判断する認証判断ステップと、当該認証判断ステップの認証結果を上記WWWサーバ部に送付する認証送付ステップとを実行した方法である。

【0013】

【発明の実施の形態】実施の形態1. 以下、この発明のホームページアクセス制御装置およびホームページアクセス制御方法の実施の形態1を説明する。図1は、実施の形態1のホームページアクセス制御装置の構成を示す構成図である。図1において、101はユーザがホームページにアクセスするためのユーザ端末部である。102は上記ホームページを表示するWWWブラウザである。103は特定ユーザのみに公開されるホームページにアクセスするために、WWWサーバ部106から上記

ユーザ端末部 101 にダウンロードされ、上記 WWW ブラウザ 102 に表示された認証ページであり、この認証ページ 103 は上記ユーザがアクセスを所望する非公開のホームページに対応するページ ID が設定されている。105 は上記ユーザの認証情報を取得する認証情報取得部であり、例えば、キーボード、指紋読み取り装置等で構成され、ここでは、ユーザ ID、パスワード、指紋情報の認証情報を取得する。104 は上記認証ページ 103 に定義され、上記 WWW サーバ部 106 から上記ユーザ端末部 101 にダウンロードされた認証画面処理部であり、上記認証情報取得部 105 が取得した認証情報と上記ユーザ所望のホームページのページ ID とを後述する WWW サーバ部 106 に送付する。

【0014】106 は上記ホームページを公開する WWW サーバ部である。107 は所定のグループにグループ化され、特定ユーザのみに公開される複数のホームページが蓄積された非公開ホームページ蓄積部である。上記ホームページは例えば電子ファイルでなる。109 は上記複数のホームページのそれぞれのページ ID と上記ホームページがそれぞれ属するグループのアクセス制御 ID とが対応づけられて格納された非公開ホームページ管理情報蓄積部であり、ここでは、さらに上記非公開ホームページ蓄積部 107 にホームページが存在するパス名が上記ホームページのページ ID に対応づけられて格納されている。

【0015】108 は上記ユーザ端末部 101 の認証画面処理部 104 から送付された上記ユーザ所望のホームページのページ ID と上記ユーザの認証情報とを受け付け、上記非公開ホームページ管理情報蓄積部 109 から上記ユーザ所望のホームページのページ ID に対応づけられた上記アクセス制御 ID を検出し、当該検出したアクセス制御 ID と上記ユーザの認証情報とを後述する認証クライアント部 110 に送付して認証要求し、当該認証結果が認証 OK の場合に上記非公開ホームページ管理情報蓄積部 109 から上記ページ ID に対応づけられたパス名を検出し、当該検出したパス名に従って上記非公開ホームページ蓄積部 107 から上記ユーザ所望のホームページを検出して上記ユーザ端末に送付する非公開ホームページアクセス処理部である。また、ここでは上記ユーザ端末 101 にホームページを送付する際に、当該ホームページが属するグループのアクセス制御 ID を含む認証を保証するトークンを上記ユーザ端末 101 に送付するように構成されている。

【0016】110 は上記非公開ホームページアクセス処理部から送付された上記アクセス制御 ID と上記ユーザの認証情報とを受け取り、当該アクセス制御 ID、ユーザの認証情報および認証クライアント ID を後述する認証サーバ部 112 に送付して認証要求し、当該認証結果を上記認証サーバ部 112 から受け取って上記非公開ホームページアクセス処理部 108 に送付する認証クラ

イアント部である。上記認証クライアント ID は認証クライアント部を識別する ID である。例えば、WWW サーバ部が複数ある場合は上記認証クライアント部も複数存在するため、認証クライアント ID により複数の WWW サーバを区別することができ、有効である。また、本実施の形態では、上記非公開ホームページアクセス処理部 108 と上記認証クライアント部 110 でアクセス部を構成する。

【0017】111 は上記ユーザ端末部 101 から送付された上記次のホームページのページ ID と上記アクセス制御 ID を含む上記トークンとを受け付け、上記非公開ホームページ管理情報蓄積部 109 から上記次のホームページのページ ID に対応づけられたアクセス制御 ID を検出し、当該検出したアクセス制御 ID と上記ユーザ端末部 101 から送付された上記トークンに含まれたアクセス制御 ID とを比較すると共に、上記トークンの有効性を判断し、有効である場合に上記非公開ホームページ管理情報蓄積部 109 から上記ページ ID に対応づけられたパス名を検出し、当該検出したパス名に従って上記非公開ホームページ蓄積部 107 から上記次のホームページを検出して上記ユーザ端末部 101 に送付する認証リンク部である。

【0018】112 は上記ホームページをアクセスするユーザの認証を行う認証サーバ部である。113 は上記ユーザの予め登録された認証情報を含むユーザ情報が格納された個人情報蓄積部である。114 は上記アクセス制御 ID と認証処理に用いられる認証の種類とが対応づけられて格納された認証許可情報蓄積部である。上記 WWW サーバ部 106 の認証クライアント部 110 から送付された上記アクセス制御 ID と上記ユーザの認証情報とを受け付け、上記認証許可情報蓄積部 114 から上記アクセス制御 ID に対応づけられた認証の種類を検出し、上記個人情報蓄積部 113 から上記検出した認証の種類に応じた上記ユーザの認証情報を検出し、当該検出した認証情報と上記認証クライアント部 110 から受け付けた認証情報とを比較して認証判断し、当該認証結果を上記認証クライアント部 110 に送付する認証判断部である。

【0019】次に、ホームページアクセス制御装置の動作およびホームページアクセス制御方法について説明する。ユーザは、特定ユーザのみに公開される所望のホームページにアクセスする際に、例えば、ユーザ端末部 101 に所定の URL を入力すると、上記ユーザ所望のホームページに対応するページ ID が設定された認証ページ 103 が、上記 WWW サーバ部 106 から上記ユーザ端末部 101 にダウンロードされる。そして上記認証ページ 103 に定義された認証画像処理部 104 が WWW ブラウザ 102 に認証画面を表示する。

【0020】図 2 は、上記認証画面処理部 104 が表示する画面の一例である。図 2 の画面では、上記ユーザは

認証情報としてユーザID、パスワード、指紋情報（指1本）、指紋情報（指2本）が選択可能である。

【0021】上記ユーザは、上記WWWブラウザ102に表示された認証画面を確認し、必要な認証項目を選択して、認証情報を入力する。例えば、ユーザIDやパスワードは、キーボードより入力し、指紋情報は、上記認証画面処理部104が表示した認証画面の取得ボタンを押下して入力する。また、例えば、認証情報取得部105に接続されたICカード読み取り装置に、ユーザID、パスワード、指紋情報等が記録されたICカードを

読み取らせることにより、上記認証情報を入力する。
【0022】上記ユーザの入力操作に応じて、認証情報取得部105は、上記ユーザの認証情報を取得する（認証情報取得ステップ）。例えば、上記キーボードから入力されたキーコードをユーザIDやパスワードの認証情報として取得する。また、上記認証画面処理部104の取得ボタンの位置に設置された指紋読み取り装置のセンサーが上記ユーザの押下を指紋情報として取得する。さらにまた、上記ICカード読み取り装置が上記ユーザのICカードに記憶されていたユーザID、パスワード、指紋情報等を読み取り、認証情報として取得する。

【0023】その後、上記ユーザが上記認証画面に表示された送信ボタンを押下すると、上記認証画面処理部104が、上記認証情報取得部105によって取得された認証情報と、上記認証ページ103に設定されていたページIDとを上記WWWサーバ部106上の非公開ページアクセス処理部108に送付する（認証画面処理ステップ）。すると、上記非公開ページアクセス処理部108は、上記認証情報とページIDを受け取り、認証処理を開始する。

【0024】以降の非公開文書アクセス処理部108の詳細な動作および処理について図1、図3および図4を用いて説明する。

【0025】図3は、非公開ホームページ管理情報蓄積部109に格納されたデータの一例である。図3において、301はホームページを識別するページIDである。302はホームページが属するグループを識別するアクセス制御IDであり、ここでは上記ホームページは内容によってグループ化されている。303はホームページが存在する場所（パス名）である。図3では、5つのホームページのそれぞれのページID、アクセス制御IDおよびパス名が格納されている。また、図4は、非公開ホームページアクセス処理部108の動作を示す流れ図である。

【0026】非公開文書アクセス処理部108は、まず上記認証画面処理部104より送付された上記ユーザの認証情報と上記ユーザ所望の非公開ホームページのページIDとを受け付ける（ステップ401、WWW受け付けステップ）。そして非公開ホームページ管理情報蓄積部109より、上記受け取ったページIDに対応づけられ

たアクセス制御IDを検出し取得する（ステップ402、WWW検出ステップ）。次にこのアクセス制御IDと上記ユーザの認証情報とを認証クライアント110に送付して認証処理を依頼する（ステップ403、認証要求ステップ）。

【0027】そして、上記認証クライアント110から送付された認証結果がOKであるか否かを判断する（ステップ404）。認証結果が認証OKの場合は、非公開ホームページ管理情報蓄積部109よりページIDに対応づけられたホームページが存在するパス名を検出し、当該検出したパス名に従って非公開ホームページ蓄積部107よりホームページを検出してWWWブラウザ102にそのホームページを送付する（ステップ405、WWW送付ステップ）。一方、認証結果がOKではなかった場合、すなわち認証NGであった場合は、エラーメッセージ用のホームページをWWWブラウザ102に送付する（ステップ406）。このように、認証が成功した場合は、上記ユーザ所望の非公開ホームページがWWWブラウザ102に表示されるが（WWWブラウザステップ）、認証が失敗した場合は、認証エラー、認証方法エラー等のエラーメッセージがWWWブラウザ102に表示され、上記ユーザは、非公開ホームページへアクセスすることができない。

【0028】次に、上記認証処理の詳細な動作および処理について図1、図5および図6を用いて説明する。図5は、個人情報蓄積部112に格納された認証情報を含む個人情報の一例である。図5では、認証情報としてユーザID、パスワード、指紋1本の情報、指紋2本の情報が格納されると共に、個人名称、所属、連絡先等の個人情報も格納されている。尚、ここでは、ユーザIDが個人情報のキーである。

【0029】図6は、認証許可情報蓄積部114に格納されたアクセス制御IDと認証処理に用いられる認証の種類とが対応づけられた認証許可情報の一例であり、ここでは、上記アクセス制御IDのほかに、ユーザIDおよび認証クライアントIDが格納され、上記アクセス制御ID、ユーザIDおよび認証クライアントIDの組み合わせに応じて認証に用いられる認証の種類が決定されるようになっている。

【0030】図6において、601は非公開ホームページをアクセスするユーザのユーザID、602は認証クライアント部110を識別する認証クライアントID、603は上記ユーザ所望のホームページのグループを識別するアクセス制御ID、604はユーザIDのユーザが認証クライアントIDの認証クライアントでアクセス制御IDに対するアクセス権を認証するときの認証手段、すなわち認証の種類、605は備考である。

【0031】図6の例では、user1がAclientでJINJI1に対してアクセスする時は、ユーザIDと指紋1本の情報で認証すること、user1がAclientでKEIRI1に対してアク

セスする時は、ユーザIDとパスワード情報で認証することが定義されている。すなわちこの例では、ユーザID601、認証クライアントID602およびアクセス制御ID603の組合わせによってグループ化し、そのグループに応じて認証の種類を変えることが可能となる。

【0032】まず、認証判断部115は、上記認証クライアント部110より送付された上記認証情報、上記アクセス制御IDおよび上記認証クライアントIDを受け付け（認証受け付けステップ）、認証許可情報蓄積部114から上記認証情報に含まれるユーザID、上記アクセス制御IDおよび上記認証クライアントIDに対応する認証の種類を検出する。そして、上記認証許可情報蓄積部114から検出された認証の種類に応じた認証情報を上記ユーザIDをキーとして上記個人情報蓄積部113から検出する（認証検出ステップ）。次に、上記個人情報蓄積部113から検出された認証情報と上記認証クライアント部110より受け付けた認証情報とを比較して、上記ユーザの認証を行い（認証判断ステップ）、その結果を上記認証クライアント部110に送付する（認証送付ステップ）。ここで、上記個人情報蓄積部113から検出した認証情報と上記認証クライアント部110より渡された認証情報とが一致する場合は、認証結果として認証OKを送付し、一致しない場合は、認証NGを送付する。

【0033】次に、WWW装置の全体の動作を説明する。図7は、認証処理の全体の流れを示すシーケンス図である。まず、ユーザが、特定ユーザのみに公開される所望のホームページにアクセスするために、上記所望のホームページに対応するURLをユーザ端末部101に入力すると、WWWサーバ部106から上記ユーザ所望のホームページに対応するページIDと認証画像処理部104の設定された認証ページ103が上記ユーザ端末部101に送付される。

【0034】その後、上記認証画面処理部104は、上記ユーザより入力された認証情報と上記認証ページ103に設定された上記ユーザ所望のホームページに対応するページIDとを、（非公開ホームページアクセス処理部108に送付する（シーケンス701）。すると、上記非公開ホームページアクセス処理部108は、非公開ホームページ管理情報蓄積部109より上記ページIDに対するアクセス制御IDを検出し、当該アクセス制御IDと上記ユーザより入力された認証情報とを認証クライアント110に送付し、認証を依頼する（シーケンス702）。

【0035】当該認証クライアント部110は、認証プロトコルに従って認証判断部115に認証を依頼すると共に、上記非公開ホームページアクセス処理部108から送付されたアクセス制御ID、認証情報および該認証クライアント部110に対応する認証クライアントID

を認証判断部115に送付する（シーケンス703）。当該認証判断部115は、個人情報蓄積部113と認証許可情報蓄積部114の情報をを用いて認証を行い、認証OKか認証NGかの認証結果を認証クライアント部110に送付する（シーケンス704）。

【0036】上記認証結果を受け取った認証クライアント部110は、その結果を更に上記非公開ホームページアクセス処理部108に送付する（シーケンス705）。当該非公開ホームページアクセス処理部108は、上記認証結果が認証NGの場合は、エラーメッセージ用のホームページをWWWブラウザ102に送付し、認証結果がOKの場合は、非公開ホームページ管理情報蓄積部109より上記ページIDに対するホームページの存在パス名を検出し、そのそのパス名に従って非公開ホームページ蓄積部107より上記ホームページを検出し、WWWブラウザ102に送付する。尚、このとき、このホームページからリンクされた次のホームページをアクセスするために、認証を保証する上記アクセス制御IDを含むトークンをこのホームページに設定しておく（シーケンス706）。

【0037】次に認証リンク部111の詳細動作および処理について、図8を用いて説明する。図8は、上記認証リンク部111の詳細な動作を示す流れ図である。前述のようにして認証OKとなり、上記ユーザ所望のホームページが上記WWWブラウザ102に表示された後、上記ユーザが上記ユーザ所望のホームページからリンクされた次のホームページをアクセスすると、上記認証リンク部111は、アクセス要求として上記WWWブラウザ102から送付された上記表示されたホームページに設定されたトークンと、上記ユーザ所望の次のホームページに対応したページIDとを受け付ける。（ステップ801）。

【0038】そして、上記認証リンク部111は、暗号化されているトークンの暗号を解きトークンの有効性の確認する（ステップ802）。上記トークンは、例えば、先に認証OKとなった時刻、認証OKとなったアクセス制御ID、有効性判定用の固定値等の情報を含み、当該各情報が有効と判断された場合にトークンの有効性を満足する。

【0039】次に、上記認証リンク部111は、上記トークンが有効であるか否かを判断し（ステップ803）、上記トークンが無効な場合は、アクセスエラーを表示するホームページを上記WWWブラウザ102に送付する（ステップ805）。一方、上記トークンが有効な場合は、上記ユーザ所望の次の非公開ホームページに対応したページIDに対するアクセス制御IDを上記非公開ホームページ管理情報蓄積部109より検出する（ステップ804）。そして、当該非公開ホームページ管理情報蓄積部109より検出したアクセス制御IDと、上記トークンに含まれていた認証時のアクセス制御

IDとの比較を行う（ステップ806）。

【0040】ステップ806で比較した結果、違っていた場合は、アクセスエラーを表示するホームページを上記WWWブラウザ102に送付し（ステップ805）、認証は継続されない。一方、ステップ806で比較した結果、同じであった場合は、認証が継続され、上記認証リンク部111は、上記非公開ホームページ管理情報蓄積部109から検出したページIDの存在パス名に従って上記非公開ホームページ蓄積部107よりホームページを検出し、新たなトークンを設定して、上記WWWブラウザ102に送付する（ステップ808）。このように、アクセス制御IDが一致した場合は、認証が継続され、新たに認証を行うことなく次のホームページにアクセスすることが可能であるが、トークンが無効である又はアクセス制御IDが一致しない場合は、認証は継続されず、例えば、新たに認証を行い、認証OKとならない限り次のホームページにアクセスすることができないため、ホームページアクセスに対するセキュリティを高めることができる。

【0041】図9は、特定ユーザのみに公開されるホームページをリンクをたどりながらアクセスしていく時のシーケンス図である。まず、前述のように、ユーザが所望のホームページに対応したURLを入力すると、上記ホームページのページIDと認証画面処理部104とが設定された認証ページ103がユーザ端末部101にダウンロードされる。そして、上記認証画面処理部104はユーザより入力された認証情報と上記認証ページ103に設定されているページIDとを、非公開ホームページアクセス処理部108に送付する（シーケンス701）。

【0042】当該非公開ホームページアクセス処理部108は、非公開ホームページ管理情報蓄積部109より上記送付されたページIDに対するアクセス制御IDを検出し、当該検出したアクセス制御IDと上記送付された認証情報とを認証クライアント110に送付し認証処理を依頼する（シーケンス901）。その結果、認証OKの場合、上記非公開ホームページアクセス処理部108は、非公開ホームページ蓄積部106より該当するホームページを検出し（シーケンス902）、認証を保証するアクセス制御IDを含むトークン（トークン1）を生成し（シーケンス903）、上記検出したホームページに設定してWWWブラウザ102に送付する（シーケンス904）。図9では、ページIDがpage1のホームページに対して、page1.htmlの電子ファイルの内容を送付している。

【0043】次に、page1.htmlからのリンクによりページIDがpage2であるホームページへのアクセス依頼が認証リンク部111に届く。このときpage1.htmlに設定されていたトークン（トークン1）も送付される（シーケンス905）。すると、認証リンク部111は、上記

トークンを解読して（シーケンス906）トークンの有効性を確認する。そしてpage2のアクセス制御IDとトークン1に含まれるアクセス制御ID、すなわちpage1のアクセス制御IDをチェックして、上記page1のアクセス制御IDと上記page2のアクセス制御IDの継続性を確認する（シーケンス907）。上記page1とpage2のアクセス制御IDが一致し、トークンに異常がない場合は、上記page2のホームページを非公開ホームページ蓄積部107より検出し（シーケンス908）、新たなトークン（トークン2）を生成する（シーケンス909）。そして、上記page2のホームページの電子ファイルであるpage2.htmlに上記生成したトークンを設定してWWWブラウザ102に送付する（シーケンス910）。

【0044】以上のように本実施の形態によれば、複数のホームページが当該ホームページの内容に応じてアクセス制御IDによりグループ化され、該アクセス制御IDと認証に用いられるユーザID、パスワード、指紋情報などの認証の種類とが対応づけられて格納された認証許可情報蓄積部を用いたことにより、アクセス可能なユーザからの認証判断を行う際に、上記グループのアクセス制御IDに応じて認証の種類を変更でき、例えば、ホームページの秘密性の度合に応じて適切な認証の種類で認証判断を行うことが可能となる。また、上記アクセス制御IDに応じて認証の種類が決定されるので、例えば、複数のWWWサーバ部に複数のホームページがそれぞれ存在する場合でも、上記複数のホームページへのアクセスに対する認証処理を一つの認証サーバ部で統一的に処理することが可能となり、ホームページへのアクセス制御機構の開発を高率化することが可能となる。

【0045】また、上記認証許可情報蓄積部が、上記アクセス制御ID、ユーザIDおよび認証クライアントIDの組み合わせに応じて認証に用いられる認証の種類が決定されることにより、より詳細にグループを分類することができるので、システム運用形態に応じてより適切な認証の種類で認証判断を行うことが可能となる。

【0046】また、非公開ホームページアクセス処理部がユーザ端末にホームページを送付する際に当該ホームページが属するグループのアクセス制御IDを上記ユーザ端末に送付し、認証リンク部が上記アクセス制御IDと上記ホームページにリンクされたユーザ所望の次のホームページのアクセス制御IDとを比較して認証の継続を判断し、一致する場合、すなわち認証が継続している場合に上記次のホームページを上記ユーザ端末部に送付することにより、ユーザが別のホームページにアクセスする度に上記ユーザの認証情報による認証を行う必要がないため、ユーザの操作性を向上することが可能となる。また、トークンが無効である又はアクセス制御IDが一致しない場合、すなわち先に認証OKとなったアクセス制御IDと異なるアクセス制御IDに属するホーム

ページをアクセスする場合は、認証は継続していないとし、例えば、新たに認証を行い、認証OKとならない限り次のホームページにアクセスすることができないため、ホームページアクセスに対するセキュリティを高めることが可能となる。

【0047】なお、本実施の形態では、認証判断部が個人情報蓄積部を検出する際にユーザIDをキーとしたが、上記キーは、ユーザを一意に決定できるものであれば良く、上記ユーザIDに限定されるものではない。例えば、認証クライアント部から送付されたユーザIDが未定義であっても、ユーザを一意に決定できる指紋情報からまずユーザIDを確定した後、同様の処理を行うことも可能である。

【0048】

【発明の効果】以上のように、この発明のホームページアクセス制御装置によれば、ホームページを公開するWWWサーバ部と上記ホームページをアクセスするユーザ端末部と上記ホームページをアクセスするユーザの認証を行う認証サーバ部で構成されるものにおいて、上記ユーザ端末部は、上記ホームページを表示するWWWブラウザと、上記ユーザの認証情報を取得する認証情報取得部と、当該認証情報取得部が取得した認証情報と上記ユーザ所望のホームページのページIDとを上記WWWサーバ部に送付する認証画面処理部とを有し、上記WWWサーバ部は、所定のグループにグループ化され、特定ユーザのみに公開される複数のホームページが蓄積された非公開ホームページ蓄積部と、上記複数のホームページのそれぞれのページIDと上記ホームページがそれぞれ属するグループのアクセス制御IDとが対応づけられて格納された非公開ホームページ管理情報蓄積部と、上記ユーザ端末部から送付された上記ユーザ所望のホームページのページIDと上記ユーザの認証情報とを受け付け、上記非公開ホームページ管理情報蓄積部から上記ユーザ所望のホームページのページIDに対応づけられた上記アクセス制御IDを検出し、当該検出したアクセス制御IDと上記ユーザの認証情報とを上記認証サーバ部に送付して認証要求し、当該認証結果が認証OKの場合に上記非公開ホームページ蓄積部から上記ユーザ所望のホームページを検出して上記ユーザ端末に送付するアクセス部とを有し、上記認証サーバ部は、上記ユーザの予め登録された認証情報が格納された個人情報蓄積部と、上記アクセス制御IDと認証処理に用いられる認証の種類とが対応づけられて格納された認証許可情報蓄積部と、上記WWWサーバ部から送付された上記アクセス制御IDと上記ユーザの認証情報とを受け付け、上記認証許可情報蓄積部から上記アクセス制御IDに対応づけられた認証の種類を検出し、上記個人情報蓄積部から上記検出した認証の種類に応じた上記ユーザの認証情報を検出し、当該検出した認証情報と上記WWWサーバ部から受け付けた認証情報とを比較して認証判断し、当該認証

結果を上記WWWサーバ部に送付する認証判断部とを有したことにより、アクセス可能なユーザの認証判断を行う際に、上記グループのアクセス制御IDに応じて認証の種類を変更でき、例えば、ホームページの秘密性の度合に応じて適切な認証の種類で認証判断を行うことが可能となる。また、上記アクセス制御IDに応じて認証の種類が決定されるので、例えば、複数のWWWサーバ部に複数のホームページがそれぞれ存在する場合でも、上記複数のホームページへのアクセスに対する認証処理を一つの認証サーバ部で統一的に処理することが可能となり、ホームページへのアクセス制御機構の開発を高率化することが可能となるという効果がある。

【0049】また、次の発明のホームページアクセス制御装置によれば、上記WWWサーバ部の上記アクセス部は、上記ユーザ端末にホームページを送付する際に当該ホームページが属するグループのアクセス制御IDを上記ユーザ端末に送付するように構成され、上記ユーザ端末部は、上記アクセス部から送付されたホームページにリンクされた上記ユーザ所望の次のホームページのページIDと上記アクセス部から送付されたアクセス制御IDとを上記WWWサーバ部に送付するように構成され、さらに、上記WWWサーバ部は、上記ユーザ端末部から送付された上記次のホームページのページIDと上記アクセス制御IDとを受け付け、上記非公開ホームページ管理情報蓄積部から上記次のホームページのページIDに対応づけられたアクセス制御IDを検出し、当該検出したアクセス制御IDと上記ユーザ端末部から送付されたアクセス制御IDとを比較し、一致する場合に上記非公開ホームページ蓄積部から上記次のホームページを検出して上記ユーザ端末部に送付する認証リンク部を有したことにより、アクセス制御IDが一致しない場合、すなわち先に認証OKとなったアクセス制御IDと異なるアクセス制御IDに属するホームページをアクセスする場合は、例えば、新たに認証を行い、認証OKとならない限り次のホームページにアクセスすることができないため、ホームページアクセスに対するセキュリティを高めることが可能となるという効果がある。また、アクセス制御IDが一致した場合は、ユーザが別のホームページをアクセスする度に上記ユーザの認証情報による認証を行う必要がないため、ユーザの操作性を向上することが可能となるという効果がある。

【0050】さらにまた、次の発明のホームページアクセス制御方法によれば、ホームページを公開するWWWサーバ部と上記ホームページをアクセスするユーザ端末部と上記ホームページをアクセスするユーザの認証を行う認証サーバ部で構成されるホームページアクセス制御装置を用いた制御方法において、上記ユーザ端末部で、上記ホームページを表示するWWWブラウザステップと、上記ユーザの認証情報を取得する認証情報取得ステップと、当該認証情報取得ステップで取得した認証情報

と上記ユーザ所望のホームページのページIDとを上記WWWサーバ部に送付する認証画面処理ステップとを実行し、上記WWWサーバ部で、上記ユーザ端末部から送付された上記ユーザ所望のホームページのページIDと上記ユーザの認証情報とを受け付けるWWW受け付けステップと、所定のグループにグループ化され、特定ユーザのみに公開される複数のホームページのそれぞれのページIDと上記ホームページがそれぞれ属するグループのアクセス制御IDとが対応づけられて格納された非公開ホームページ管理情報蓄積部から上記ユーザ所望のホームページのページIDに対応づけられた上記アクセス制御IDを検出するWWW検出ステップと、当該WWW検出ステップで検出したアクセス制御IDと上記ユーザの認証情報とを上記認証サーバ部に送付して認証要求する認証要求ステップと、上記認証の結果が認証OKの場合に上記ユーザ所望のホームページを上記非公開ホームページ蓄積部から検出して上記ユーザ端末部に送付するWWW送付ステップとを実行し、上記認証サーバ部で、上記WWWサーバ部から送付された上記アクセス制御IDと上記ユーザの認証情報とを受け付ける認証受け付けステップと、上記アクセス制御IDと認証処理に用いられる認証の種類とが対応づけられて格納された認証許可情報蓄積部から上記認証受け付けステップで受け付けたアクセス制御IDに対応づけられた認証の種類を検出し、上記ユーザの予め登録された認証情報が格納された個人情報蓄積部から上記検出された認証の種類に応じた上記ユーザの認証情報を検出する認証検出ステップと、当該認証検出ステップで検出した認証情報と上記WWWサーバ部から受け付けた認証情報とを比較して認証判断する認証判断ステップと、当該認証判断ステップの認証結果を上記WWWサーバ部に送付する認証送付ステップとを実行したことにより、アクセス可能なユーザかの認証判断を行う際に、上記グループのアクセス制御IDに応じて認証の種類を変更でき、例えば、ホームページの秘密性の度合に応じて適切な認証の種類で認証判断を行うことが可能となる。また、上記アクセス制御IDに応じて認証の種類が決定されるので、例えば、複数のWWWサーバ部に複数のホームページがそれぞれ存在する場合でも、上

【図 3】

ページID	アクセス制御ID	ホームページが存在するパス名
page1	JINJI1	C:\JINJI1\page1.html
page2	JINJI1	C:\JINJI1\page2.html
page3	JINJI1	C:\JINJI1\page3.html
page4	KEIRI1	C:\KEIRI1\page4.html
page5	KEIRI1	C:\KEIRI1\page5.html

記複数のホームページへのアクセスに対する認証処理を一つの認証サーバ部で統一的に処理することが可能となり、ホームページへのアクセス制御機構の開発を高率化することが可能となるという効果がある。

【図面の簡単な説明】

【図 1】 この発明の実施の形態 1 によるホームページアクセス制御装置を示す構成図である。

【図 2】 この発明の実施の形態 1 において認証画面処理部が表示する画面の一例を示す説明図である。

【図 3】 この発明の実施の形態 1 において非公開ホームページ管理情報蓄積部に格納されたデータの一例を示す説明図である。

【図 4】 この発明の実施の形態 1 における非公開ホームページアクセス処理部の詳細動作を示す流れ図である。

【図 5】 この発明の実施の形態 1 において個人情報蓄積部に格納されたデータの一例を示す説明図である。

【図 6】 この発明の実施の形態 1 において認証許可情報蓄積部に格納されたデータの一例を示す説明図である。

【図 7】 この発明の実施の形態 1 における認証処理の流れを説明するシーケンス図である。

【図 8】 この発明の実施の形態 1 における認証リンク部の詳細動作を示す流れ図である。

【図 9】 この発明の実施の形態 1 において非公開ホームページのリンクをたどったアクセスの制御の流れを示すシーケンス図である。

【図 10】 従来のホームページアクセス制御装置を示す構成図である。

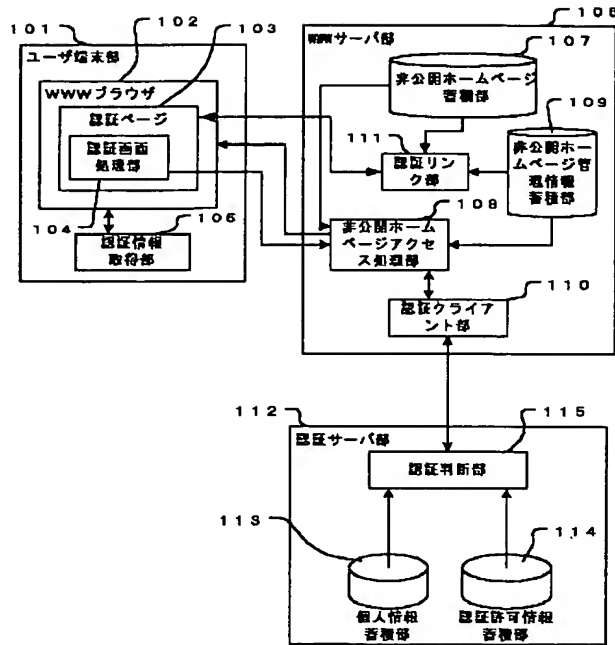
【符号の説明】

101：ユーザ端末部、102：WWWブラウザ、103：認証ページ、104：認証画面処理部、105：認証情報取得部、106：WWWサーバ部、107：非公開ホームページ蓄積部、108：非公開ホームページアクセス処理部、109：非公開ホームページ管理情報蓄積部、110：認証クライアント部、111：認証リンク部、112：認証サーバ部、113：個人情報蓄積部、114：認証許可情報蓄積部、115：認証判断部

【図 5】

ユーザID	パスワード	指紋情報 1	指紋情報 2	個人名称	所属
user1	user1pass	指紋情報へのポイント	指紋情報へのポイント	認証花子	経理

【図1】



【図2】

アクセス者認証画面

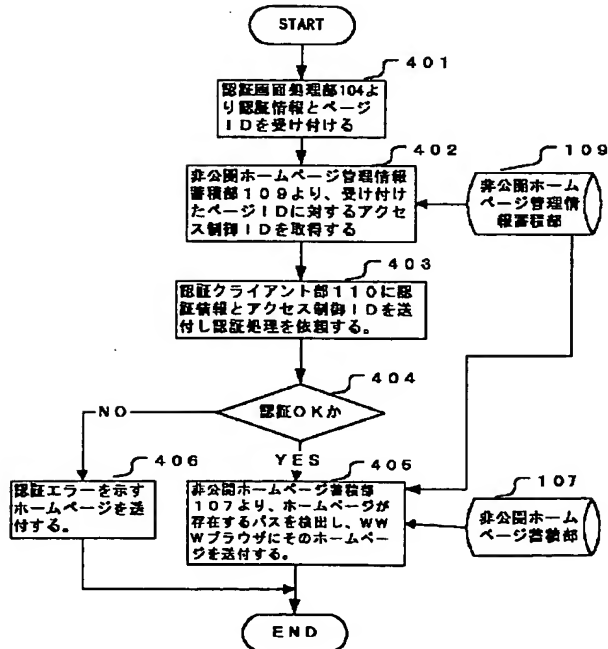
☐ ユーザ ID

☐ パスワード

☐ 指紋情報1本

☐ 指紋情報2本

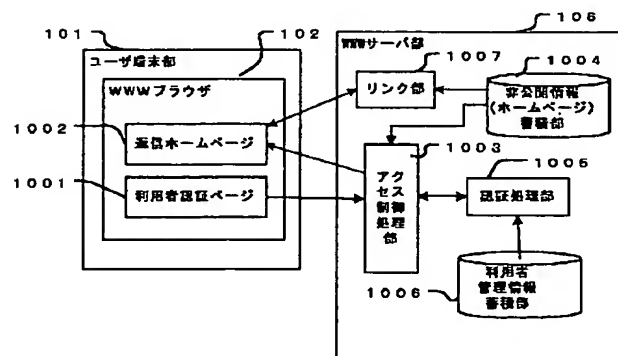
【図4】



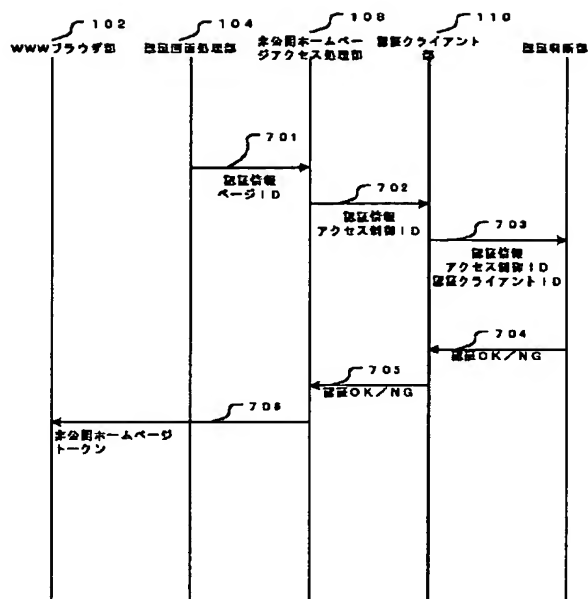
【図6】

ユーザID	認証クライアントID	アクセス制御ID	認証手段	備考
user1	AClient	JINJI1	ユーザIDと指紋情報1本	
user1	AClient	KEIRI1	ユーザIDとパスワード	

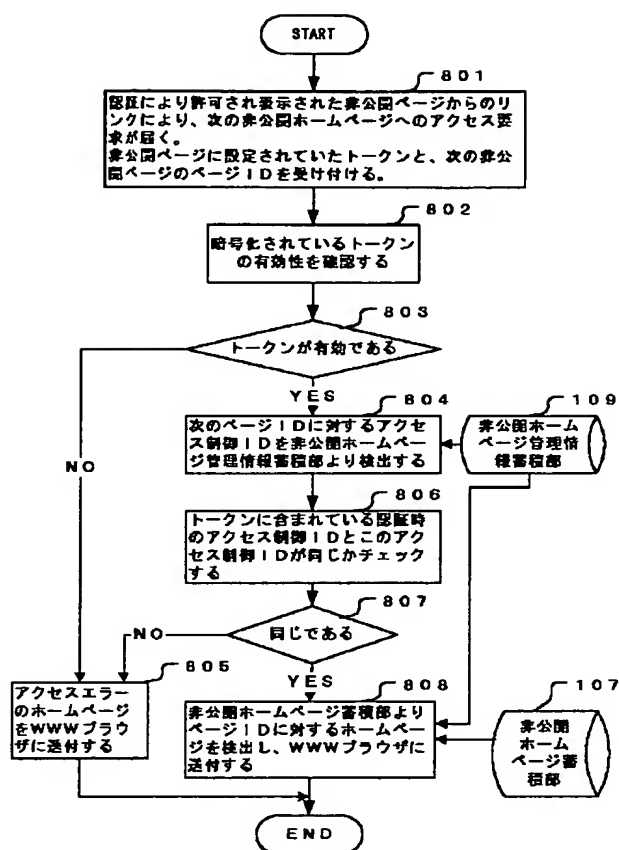
【図10】



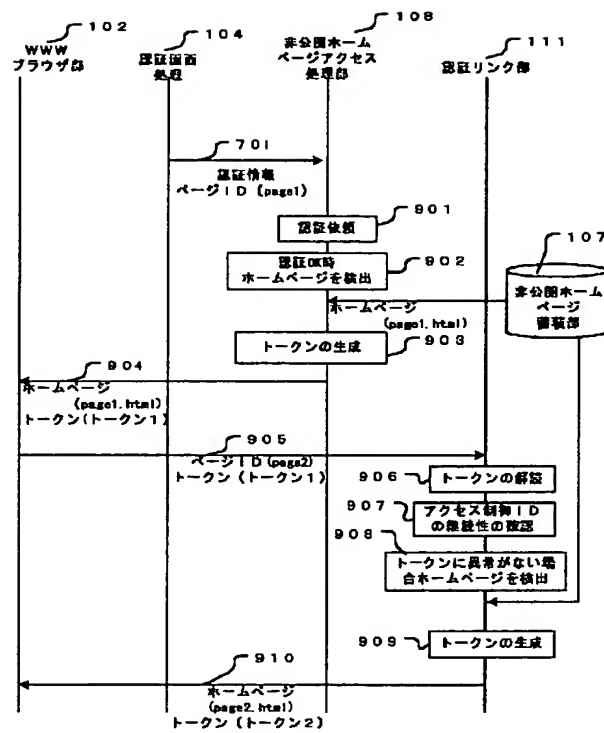
【図7】



【図8】



【図9】



フロントページの続き

(72)発明者 貞包 哲男

東京都千代田区丸の内二丁目2番3号 三
菱電機株式会社内

Fターム(参考) 5B085 AE04 AE06 AE23 BG07